PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-325249
(43)Date of publication of application : 22.11.2001

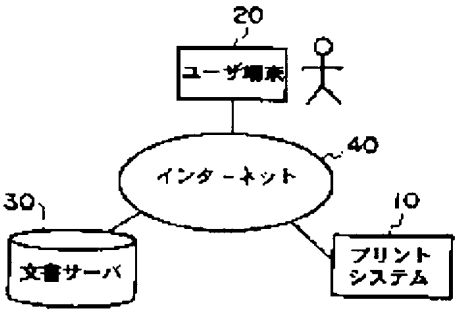
(51)Int.Cl. G06F 17/21
G06F 12/00
G06F 12/14
G06F 15/00
G06F 17/30

(21)Application number : 2000-140790
(22)Date of filing : 12.05.2000

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : OTAKE SUSUMU

(54) DOCUMENT PROVIDING DEVICE AND SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To manage the presentation of a document to users of different access rights by the constituting element unit of the document.
SOLUTION: For an HTML document stored in a document server 30, a security level is set by the constituting element unit. In the case that a user specifies a document inside the document server 30 as a printing object and instructs its printing to a print system 10, the print system 10 acquires the document from the document server 30 and further acquires the information on the security level of the user from a directory service or the like. Then, the print system 10 compares the security levels of the respective constituting elements of the acquired document with the security level of the use and judges, for the respective constituting element, whether the element can be presented to the user. Then, the element for which it is judged that the presentation is impossible is replaced with the image of a turned letter or the like and printed.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－325249
（P2001－325249A）
(43)公開日　平成13年11月22日(2001.11.22)

(51)Int.Cl.[7]		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	17/21	５７０	Ｇ０６Ｆ	17/21	５７０Ｍ	５Ｂ００９
	12/00	５３７		12/00	５３７Ａ	５Ｂ０１７
	12/14	３２０		12/14	３２０Ａ	５Ｂ０７５
	15/00	３３０		15/00	３３０Ｚ	５Ｂ０８２
	17/30	１２０		17/30	１２０Ｂ	５Ｂ０８５

審査請求　未請求　請求項の数10　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願2000－140790(P2000－140790)

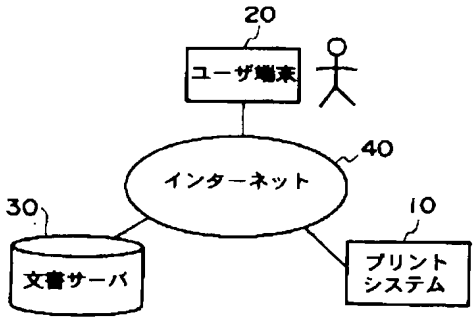
(22)出願日　平成12年５月12日(2000.5.12)

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号
(72)発明者　大竹　晋
神奈川県海老名市本郷2274番地　富士ゼロックス株式会社海老名事業所内
(74)代理人　100075258
弁理士　吉田　研二　（外２名）

Ｆターム(参考)　5B009 SA00 TB13
5B017 AA07 BA06 CA16
5B075 KK43 KK54 KK63 PQ02 UU06
5B082 GA11
5B085 AE06 BG07

(54)【発明の名称】　文書提供装置及びシステム

(57)【要約】
【課題】　アクセス権限の異なるユーザに対する文書の開示管理を、文書の構成要素単位で行えるようにする。
【解決手段】　文書サーバ３０に格納されたＨＴＭＬ文書は、構成要素単位でセキュリティレベルが設定されている。ユーザがプリントシステム１０に、文書サーバ３０内の文書を印刷対象に指定して印刷指示を行った場合、プリントシステム１０は、文書サーバ３０からその文書を取得するとともに、ディレクトリサービスなどからそのユーザのセキュリティレベルの情報を取得する。そして、プリントシステム１０は、取得した文書の各構成要素のセキュリティレベルとそのユーザのセキュリティレベルとを比較し、各構成要素ごとに、その要素がそのユーザに開示可能か否かを判定する。そして、開示不可と判定した要素については伏せ字等の画像に置き換えて印刷する。



1

【特許請求の範囲】

【請求項１】　ユーザから文書取得命令を受信する命令受信手段と、
前記文書取得命令を発行した前記ユーザのセキュリティ情報を取得するユーザセキュリティ取得手段と、
前記文書取得命令にて指定された文書を取得する文書取得手段と、
取得した文書の各構成要素ごとに、その構成要素のセキュリティ情報を取得する文書要素セキュリティ取得手段と、
前記取得した文書の各構成要素ごとに、その構成要素のセキュリティ情報と前記ユーザのセキュリティ情報との関係からその構成要素のそのユーザに対する開示可能性を判定する開示判定手段と、
前記各構成要素ごとの開示可能性の判定の結果に応じて、前記取得した文書を編集して出力する出力制御手段と、
を備える文書提供装置。

【請求項２】　前記文書取得手段は、前記文書取得命令にて指定された文書をネットワークを介して取得することを特徴とする請求項１記載の文書提供装置。

【請求項３】　前記出力制御手段は、前記開示判定手段で開示不可能と判定された構成要素については、予め登録した置換情報に置き換えて出力することを特徴とする請求項１記載の文書提供装置。

【請求項４】　前記出力制御手段は、前記構成要素の種類ごとに、前記置換情報を生成するための情報を記憶しておき、前記構成要素ごとにその種類に応じた置換情報に置き換えることを特徴とする請求項３記載の文書提供装置。

【請求項５】　前記ユーザのセキュリティ情報と前記文書の構成要素のセキュリティ情報との関係に基づく開示可能性の判定の基準となる判定ルールを保持する手段を備え、前記開示判定手段は、この判定ルールを参照して開示可能性の判定を行うことを特徴とする請求項１記載の文書提供装置。

【請求項６】　前記文書取得命令の発行者であるユーザの電子証明書を取得する手段と、
前記文書取得命令に対応して取得した電子証明書の正当性を検証する手段と、
を備え、
前記文書取得手段は、前記ユーザの電子証明書が正当であると検証できた場合に、その文書取得命令にて指定された文書を保持するサーバに対し、その電子証明書を用いて前記ユーザの代理としてアクセスしてその文書を取得する、請求項１記載の文書出力装置。

【請求項７】　前記文書取得命令の発行者であるユーザの電子証明書を取得し記憶する手段と、
前記文書取得命令に関する処理において発生したイベントに関し、前記発行者であるユーザに通知を行う手段であって、そのユーザの電子証明書が前記証明書記憶手段に記憶されている場合には、その電子証明書の情報を用いて通知内容を暗号化した上で通知するイベント通知手段と、
を備える請求項１記載の文書提供装置。

【請求項８】　構成要素単位でセキュリティ情報が設定された文書を保持する文書サーバと、
ユーザからの文書取得要求に応じて前記文書サーバから文書を取得し、この文書の各構成要素のセキュリティレベルとそのユーザのセキュリティレベルとの関係からそれら各構成要素ごとに開示の可否を判定し、その判定結果に応じて開示できない構成要素については所定の秘匿処理を施して前記ユーザに提供する文書提供装置と、
を含む文書提供システム。

【請求項９】　各ユーザのセキュリティレベルを管理するディレクトリサービスを備え、
前記文書提供装置はこのディレクトリサービスから前記ユーザのセキュリティレベルを取得することを特徴とする請求項８記載の文書提供システム。

【請求項１０】　前記文書提供装置は、ユーザから電子証明書を受信し、この電子証明書から当該ユーザのセキュリティレベルを取得することを特徴とする請求項８記載の文書提供システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ユーザからの要求に応じて文書出力を行う文書提供装置に関する。

【０００２】

【従来の技術】ＬＡＮ上の文書サーバやインターネット上のＷｅｂ（ウェブ）サーバなど、ユーザに電子文書を提供するシステムが普及している。また、近年、ユーザから直接又はネットワークを介して文書のＵＲＬの指定を受け、このＵＲＬを用いてインターネット上のその文書を取得して印刷する機能を持つプリンタも開発されている。

【０００３】このようなシステムにおいては、文書開示に関するセキュリティ管理が重要な問題となる。例えば、企業活動において作成され保存される文書は、広く一般に公開する文書から高度な機密を要する文書まで、セキュリティのレベルが多岐にわたる。このような電子文書のセキュリティ管理は、従来例えば、個々のユーザやユーザグループに対し、文書ファイル単位やフォルダ（ディレクトリ）単位でアクセス権を設定することにより行われていた。また、Ｗｅｂページ（ＨＴＭＬ文書）へのアクセスを受け付ける際に、パスワード入力などによりユーザ認証を行って、予め許可されたものしかＨＴＭＬ文書を閲覧できないようにすることも広く行われている。

【０００４】また、特開平９－２９３０３６号公報には、クライアント装置からプリントサーバに印刷操作指

示を発行する際、発行者のユーザ名と共に身分証明書データを作成してプリントサーバに送信し、プリントサーバ側でこの身分証明書データに基づきユーザ認証を行うことにより、印刷ジョブに関する操作指示の実行可否を決定するシステムが開示されている。このシステムでは、操作指示のプロトコルに依存しない身分証明書データを用いることにより、マルチプロトコル対応プリンタにおいてユーザ認証を可能にしている。

【０００５】

【発明が解決しようとする課題】しかしながら、上記各従来技術では、ユーザ認証によるセキュリティの管理は、文書ファイルやフォルダ、あるいは印刷ジョブの単位でしか行うことができない。

【０００６】ところが、一般に１つの文書には様々な内容の記事、図版、写真などが含まれており、これらそれぞれが固有の意義を有している。極端な場合、企業名や製品の商標などの固有名詞等、個々の語句だけでも秘密保護上重要な意味を持つ場合がある。したがって、文書中に１つでも極秘の記事や図版、語句などがあれば、文書全体を極秘扱いにして閲覧を制限するのが一般的である。また、例えば同じ内容の文書を、社内イントラネット、取引先企業との間のエクストラネット、インターネットによる一般公開、などと情報開示レベルの異なる複数の対象に開示しようとする場合、従来は、開示対象ごとに開示可能レベルを考慮してＷｅｂページを個別作成しなければならなかった。

【０００７】このように従来は、文書単位で開示、非開示を判定するか、あるいは同内容の文書について各開示対象向けのバージョンを予め作成するかしかない。前者は文書の有効利用の面で十分なものとは言えず、後者は文書の有効利用はできるが手間がかかるという問題があった。

【０００８】本発明は、このような問題に鑑みなされたものであり、文書開示のセキュリティ管理を、少ない手間で、きめ細かく行える装置及びシステムを提供することを目的とする。

【０００９】

【課題を解決するための手段】上記目的を達成するため、本発明に係る文書提供装置は、ユーザから文書取得命令を受信する命令受信手段と、前記文書取得命令を発行した前記ユーザのセキュリティ情報を取得するユーザセキュリティ取得手段と、前記文書取得命令にて指定された文書を取得する文書取得手段と、取得した文書の各構成要素ごとに、その構成要素のセキュリティ情報を取得する文書要素セキュリティ取得手段と、前記取得した文書の各構成要素ごとに、その構成要素のセキュリティ情報と前記ユーザのセキュリティ情報との関係からその構成要素のそのユーザに対する開示可能性を判定する開示判定手段と、前記各構成要素ごとの開示可能性の判定の結果に応じて、前記取得した文書を編集して出力する出力制御手段とを備える。

【００１０】この構成によれば、文書提供装置は、ユーザに対する開示可能性を、文書の構成要素単位で判定した上で、必要な編集を加えて出力することができる。なお、この文書提供装置は、例えば、提供する文書を自分で保持・管理していてもよいし、提供する文書をネットワーク上の他のサーバから取得して、必要な編集を加えるような方式でもよい。

【００１１】また、好適な態様では、出力制御手段は、前記開示判定手段で開示不可能と判定された構成要素については、予め登録した置換情報に置き換えて出力する。更に好適には、出力制御手段は、前記構成要素の種類ごとに、前記置換情報を生成するための情報を記憶しておき、前記構成要素ごとにその種類に応じた置換情報に置き換える。

【００１２】また、別の好適な態様では、ユーザのセキュリティ情報と文書構成要素のセキュリティ情報との関係に基づく開示可能性の判定の基準となる判定ルールを保持する手段を備え、前記開示判定手段は、この判定ルールを参照して開示可能性の判定を行う。この態様では、個々のユーザや文書構成要素のセキュリティ情報を変更しなくても、開示ルールを変更することにより、開示範囲を変更することができる。

【００１３】また、別の好適な態様では、文書提供装置は、前記文書取得命令の発行者であるユーザの電子証明書を取得する手段と、前記文書取得命令に対応して取得した電子証明書の正当性を検証する手段とを備え、前記文書取得手段は、前記ユーザの電子証明書が正当であると検証できた場合に、その文書取得命令にて指定された文書を保持するサーバに対し、その電子証明書を用いて前記ユーザの代理としてアクセスしてその文書を取得する。この態様では、文書提供装置が文書の保管場所から文書を取得する際に、ユーザの電子証明書を用いてセキュア通信方式で文書を代理取得することができる。

【００１４】また、別の好適な態様では、文書提供装置は、前記文書取得命令の発行者であるユーザの電子証明書を取得し記憶する手段と、前記文書取得命令に関する処理において発生したイベントに関し、前記発行者であるユーザに通知を行う手段であって、そのユーザの電子証明書が前記証明書記憶手段に記憶されている場合には、その電子証明書の情報を用いて通知内容を暗号化した上で通知するイベント通知手段と、を備える。この態様では、文書提供装置からユーザへの通知の内容の秘密を保護することができる。

【００１５】また、本発明に係る文書提供システムは、構成要素単位でセキュリティ情報が設定された文書を保持する文書サーバと、ユーザからの文書取得要求に応じて前記文書サーバから文書を取得し、この文書の各構成要素のセキュリティレベルとそのユーザのセキュリティレベルとの関係からそれら各構成要素ごとに開示の可否

を判定し、その判定結果に応じて開示できない構成要素については所定の秘匿処理を施して前記ユーザに提供する文書提供装置とを備える。

【００１６】このシステムでは、ユーザに対して文書を提供する際に、文書の構成要素単位で開示可否を判定し、開示できない要素については所定の秘匿処理を施した上で出力することができる。このシステムによれば、同一内容の文書について、ユーザのセキュリティ（アクセス権限）のレベルごとに開示範囲を変えた複数のバージョンを作成し保持しておく必要がない。

【００１７】

【発明の実施の形態】以下、本発明の実施の形態（以下実施形態という）について、図面に基づいて説明する。

【００１８】図１は、本発明の実施形態の全体的なシステム構成を示す図である。本実施形態では、プルプリント機能を持つプリントシステム１０を、遠隔のユーザ端末２０からの指示により操作して印刷する場合を例にとって説明する。プルプリント機能とは、ユーザから印刷対象の文書ファイルのアドレス（ＵＲＩ（uniform resource identifier）等）を受け付け、このアドレスを用いてその文書ファイルを取得して印刷する機能である。

【００１９】ユーザ端末２０は、ＰＣ（パーソナルコンピュータ）や携帯情報端末、携帯電話などである。文書サーバ３０は、例えばＷｅｂ（WWW：ワールド・ワイド・ウェブ）サーバや匿名ＦＴＰサーバなど、ユーザに対して文書等のファイルを提供するサーバである。

【００２０】プリントシステム１０は、ＩＰＰ／１．０（internet Printing protocol：|RFC2565|,|RFC2566|）に規定されているPrint-URI命令などを受け付ける機能を備えている。ユーザ端末２０からPrint-URI命令によりＵＲＩを指定して印刷を指示すると、プリントシステム１０は、インターネット４０を介してそのＵＲＩが示す文書を格納した文書サーバ３０にアクセスし、その文書のファイルを取得して印刷する。このとき、本実施形態のプリントシステム１０は、取得した文書の開示可能性を、記事や図版、語句などの構成要素単位で判定し、印刷要求元のユーザに対して開示不可能な構成要素について所定の秘匿処理を行った上で印刷処理を行う。

【００２１】文書構成要素の開示可否の判定は、当該構成要素のセキュリティレベルと印刷要求元のユーザのセキュリティレベルとの比較に基づき行う。このため、文書には構成要素単位でセキュリティレベルが設定可能となっている。そして、プリントシステム１０は、それら各構成要素のセキュリティレベルと、印刷要求元のユーザのセキュリティレベルとを取得する機構を備える。

【００２２】図２を参照して、文書の構成要素単位でのセキュリティレベルの設定の方法の一例について説明する。

【００２３】図２は、構成要素単位でセキュリティレベルが設定された文書の一例である。この例は、ＨＴＭＬ文書の場合の例であり、文書の構成要素へのセキュリティレベルの設定に、２つの方式を用いている。

【００２４】第一の方式は、ＨＴＭＬの文書要素の単位でセキュリティレベルを設定する場合に用いる方式であり、その文書要素を表す既存のタグに、Publicityパラメータを付加するというものである。図２の例では、たとえば文書本体を表す＜BODY＞タグ５００のタグ名「BODY」の後に、「Publicity="level 1"」の形でパラメータが設定されている。これにより文書要素「BODY」に対し、“level 1”という文字列で表されるセキュリティレベルが設定されたことになる。このような方式で、タグ名に続いてPublicityパラメータを記述することにより、例示した「BODY」タグだけでなく、ＨＴＭＬで定められるすべてのタグ（すなわち文書要素）に対してセキュリティレベルを指定できる。

【００２５】セキュリティレベル設定の第二の方式は、１つの文書要素中の語句等に対してセキュリティレベルを設定する場合の方式である。この方式では、レベル設定用に定めた＜Publicity＞タグで対象となる文字列等を挟むことにより、その文字列等にセキュリティレベルを設定する。例えば、図２の例では、ＨＴＭＬ文書のテキスト部分の“松竹梅”という文字列５１５の前後に、＜Publicity＞タグの開始タグ５１０ａ（＜Publicity Level="level3"＞）と終了タグ５１０ｂ（＜/Publicity＞）が設定されている。セキュリティレベルは、そのタグの中のLevelパラメータ（例えば「Level="level 3"」）に設定される。ここでLevelパラメータとして指定可能な値の集合は、前述の第一の方式におけるPublicityパラメータの場合と同じである。

【００２６】このように、図２に示した例では、ＨＴＭＬ文書の文書要素、及びその中の語句等のレベルの要素に対し、セキュリティレベルが設定できる。文書作成者は、このような方法により、文書の各構成要素ごとに個別にセキュリティレベルを設定することができる。文書サーバ３０には、このような文書が格納されている。

【００２７】プリントシステム１０は、図２に示したような文書を取得した場合、その文書をパーズする際に、Publicityパラメータや＜Publicity＞タグを検知すると、そのパラメータやタグが付された文書要素又は語句等について、そのパラメータ等に示すセキュリティレベルが指定されているものと判断する。

【００２８】ユーザのセキュリティレベルは、例えば、オフィスその他の組織のシステム管理者によって付与される。各ユーザのセキュリティレベルの情報は、プリントシステム１０に保持させてもよいが、プリントシステム１０とは別のサーバ装置で集中管理してネットワーク上の各プリントシステム１０から参照できるようにすれば、個々のプリントシステムのコストやセキュリティレベルに関する保守コストの面で有利である。このようなアプローチの１つとして、ネットワーク上のディレクト

リサービスにてセキュリティレベル情報を管理する方式が可能である。

【００２９】次に、図３を参照して、プリントシステム１０の詳細な構成とこのシステムによる印刷処理の手順を説明する。図３のシステムは、ジョブの管理や印刷可能形式への展開を行うプリントサーバ１００と、用紙への印刷処理を行うプリントエンジン１５０から構成される。なお、図３では、印刷対象文書のデータの流れは、基端に黒丸印のついた実線矢印で、機能モジュール間のメッセージの流れは破線矢印で示している。

【００３０】プリントサーバ１００の各機能モジュールでは、ジョブ受信部１０２はユーザからの印刷指示（ジョブ）を受信する。ユーザからのジョブには、印刷対象の文書データが付属する場合と、印刷対象文書のＵＲＩが指定されている場合とがある。後者の場合、文書取得部１０４が、そのＵＲＩを用いて印刷対象文書を、ネットワーク上の当該文書の格納場所から取得する。受信したジョブや、文書取得部１０４が取得した文書のデータはスプールバッファ１０６に蓄積される。文書解析部１０８は、スプールバッファ１０６から文書データを取得し、その文書データを解析して、プリントエンジン１５０にて印字可能なビットマップデータに展開する。また、文書解析部１０８は、印刷対象文書の解析の際に、文書要素や語句に対するセキュリティレベルの設定を検出し、その情報をセキュリティ評価部１３０に渡して評価を求める。セキュリティ評価部１３０は、印刷ジョブ発行元のユーザのセキュリティレベルを取得し、文書解析部１０８から得た文書の各構成要素のセキュリティレベルと比較することにより、それら各構成要素が当該ユーザに対して開示可能か否かを判定する。この判定結果は、文書解析部１０８に返される。文書解析部１０８は、この判定結果に応じ、開示可能と判定された構成要素はそのままビットマップ画像に展開し、開示不可と判定された構成要素については、伏せ字にしたり黒塗りにしたり等、予め設定した画像に置き換えることにより、元の文書から印刷可能なビットマップデータを構成する。得られたビットマップデータはページバッファ１１０に一旦保持され、出力制御部１１２により順次プリントエンジン１５０に対して供給される。

【００３１】ジョブ制御部１１４は、受信したジョブ群の処理の流れを管理する。タッチパネル１１８は、ユーザからローカルに指示を受け付けるための装置であり、表示したユーザインタフェース画面に対するユーザからの指示を取得する。入力制御部１１６は、タッチパネル１１８の制御を行ってユーザからの指示を取得し、サーバ１００内の各モジュールに伝達する。通知部１２２は、プリントサーバ１００内で発生したイベント等に関する通知を、所定の通知先に対して発する。通知部１２２が発するイベント通知には、ジョブ完了や用紙切れなどジョブに関するイベントの通知や、紙詰まりやトナー切れなどプリントシステム１０のイベントの通知などがある。これら通知は電子メールなどの形で通知先に通知される。通知先は、予めプリントシステム１０に設定されている人（例えばシステム管理者）や、印刷ジョブ指示時にユーザが指定した通知先などである。

【００３２】なお、以上に説明したプリントサーバ１００の各機能モジュールは、タスク間通信バス１２０を介して通信を行い、処理を実行していく。

【００３３】次に、図４を参照して、本実施形態のプリントシステム１０を用いた印刷処理について説明する。

【００３４】Ｓ１０：まずユーザがユーザ端末２０からプリントシステム１０に対し、文書サーバ３０に蓄積されている文書の印刷指示を送信する。この指示には、例えばＩＰＰ／１．０で定められているPrint-URI命令が用いられる。この命令では、印刷対象文書のＵＲＩを、document-uriIPPオペレーションアトリビュートとして指定することができる。このアトリビュートには、例えば次のような値が指定される。

http://"document-server's address"/path/document.html

【００３５】ここで"document-server's address"には、文書サーバのアドレスを表す文字列が記述される。また、この命令のアトリビュートの一つであるrequest-user-name属性には、この命令の発行者名が格納されている。一般に、ネットワーク上のディレクトリサービスにログインしているユーザであれば、その属性には、ディスティングイッシュド・ネームと呼ばれる当該命令発行者のユーザ名が格納される。

【００３６】Ｓ１２：ユーザから印刷指示を受信したプリントシステム１０のジョブ受信部１０２は、ジョブ制御部１１４に対して当該指示に対応するジョブの生成を依頼する。

【００３７】Ｓ１４：ジョブ制御部１１４は、依頼されたジョブを生成し、そのジョブをスプールバッファ１０６へ書き込む準備が完了したときに、文書取得部１０４に対し、印刷対象文書のＵＲＩを指定して取得依頼を行う。

【００３８】Ｓ１６：この依頼を受けた文書取得部１０４は、document-uriIPPオペレーションアトリビュートで指定されたＵＲＩのスキームであるＨＴＴＰプロトコルを使用して、その印刷対象のＨＴＭＬ文書を格納場所である文書サーバ３０から取得し、スプールバッファ１０６への書き込みを行う。

【００３９】Ｓ１８：スプールバッファ１０６への文書の書き込みが終了すると、ジョブ制御部１１４は、文書解析部１０８に対してその文書の解析を開始させる。すると、文書解析部１０８は、ＨＴＭＬ文書の解析を開始し、印刷可能なビットマップデータへ展開していく。

【００４０】Ｓ２０：この解析処理において、ＨＴＭＬ文書からPublicityタグ又はパラメータを検出した場

合、文書解析部１０８は、そのタグ又はパラメータに示されたセキュリティレベルの値をセキュリティレベル評価部１３０に渡し、当該タグ又はパラメータに対応する構成要素の開示可否の評価を行わせる。セキュリティレベル評価部１３０は、その構成要素のセキュリティレベルを、ネットワーク上のディレクトリサービスから取得したユーザのセキュリティレベルと比較し、その構成要素が開示可能か否かを判定し、その結果を文書解析部１０８に渡す。構成要素が開示可能と判定された場合は、文書解析部１０８は、その構成要素をＨＴＭＬ文書の記述に従ってビットマップイメージへ展開する。一方、構成要素が開示不可と判定された場合は、文書解析部１０８は、その構成要素に対し、予め設定されたセキュリティポリシーに従った秘匿処理を施す。秘匿処理には、例えばその構成要素が文字列の場合は、個々の文字を「＊」などと予め設定しておいた伏せ字に置き換えるなどがある。また、開示不可の構成要素の部分を空白や黒塗り画像に置き換えたり、予め設定しておいた警告文や警告画像に置き換えるというポリシーも考えられる。

【００４１】このような置き換え処理では、例えば秘匿すべき要素が文字列の場合は伏せ字に、画像の場合は黒塗りになどと、構成要素の種類ごとに、置換する画像を予め登録しておくことも好適である。文書解析部１０８では、タグの記述から当該構成要素の種類を判別し、その判別結果に応じて、適切な置換画像に置き換える。

【００４２】Ｓ２２：このようにして印刷対象文書のビットマップイメージへの展開が終わると、ジョブ制御部１１４は出力制御部１１２に対してその文書の出力を指示する。これにより、ビットマップイメージがプリントエンジン１５０に供給され、用紙上に印刷される。

【００４３】このような開示セキュリティ管理により得られる図２のＨＴＭＬ文書の印刷結果の例を図５～図８に示す。これらの例では、ユーザのセキュリティレベルの値が文書構成要素のセキュリティレベル未満の場合にその文書構成要素を開示不可とし、Publicityパラメータでセキュリティ設定がなされた文書要素については組版自体を省略し、Publicityタグでセキュリティ設定された語句については伏せ字「＊」に置き換えるというセキュリティポリシーを採用しているものとする。

【００４４】図５は、セキュリティレベル０のユーザの場合の印刷結果であり、レベル１以上の文書要素は全く印刷されておらず、セキュリティレベル設定のなされていない要素のみが表示されている。図６はセキュリティレベル１のユーザの場合の印刷結果であり、レベル１以下の構成要素が表示されている。図７はセキュリティレベル２のユーザの場合の印刷結果であり、セキュリティレベル３の構成要素である語句“松竹梅”（図２参照）が伏せ字「＊＊＊」に置き換えられている。図８は、セキュリティレベル３のユーザの場合の印刷結果であり、文書のすべての要素が表示されている。

【００４５】以上説明したように、本実施形態のプリントシステム１０によれば、文書の構成要素単位で、印刷要求元のユーザに対して開示可能か否かを判定し、開示不可のものを秘匿して印刷することができる。したがって、本実施形態によれば、セキュリティレベルの異なる複数のユーザに対して、単一の文書を用意しておくだけで、各ユーザのセキュリティレベルに応じた開示管理を行うことができる。

【００４６】＜変形例１＞以上の例では、ユーザのセキュリティレベルと文書構成要素のセキュリティレベルを単純に数値比較することにより開示可能性を判断した。この場合、各セキュリティレベルのユーザに対して開示する文書要素の範囲を変更する場合には、個々の構成要素のセキュリティレベルの値を変更するか、あるいは個々のユーザのセキュリティレベルの値を変更するかのいずれかが必要となる。これに対し、この変形例では、開示範囲の変更をより容易にするための仕組みの例を説明する。

【００４７】この変形例では、ユーザと文書要素のセキュリティレベルの解釈及び比較のルールをセキュリティレベル評価部１３０に登録する。セキュリティレベル評価部１３０は、このルールを参照して、ユーザと文書構成要素のセキュリティレベルを比較し、開示可否を判定する。

【００４８】例えば、ある組織においてプロジェクトＡというプロジェクトが進行中であり、そのプロジェクトＡに関する文書を文書サーバ３０に登録してプロジェクト関係者に開示するという状況を考える。ここでプロジェクトの構成人員が、アルバイト、正社員、プロジェクトＡの担当社員、プロジェクトＡの担当役員、の４段階のレベルに分類できるものとし、これらのレベルが、当該人員（ユーザ）の文書開示レベル（セキュリティレベル）に対応しているものとする。

【００４９】このような組織において、ディレクトリサービスにアルバイト、正社員、プロジェクトＡ担当社員、プロジェクトＡ担当役員というユーザオブジェクトを作成する。この場合、これら４種のオブジェクトが各ユーザのセキュリティレベルを表し、各ユーザはそれら４種のユーザオブジェクトのいずれかに対応づけられる。また、個々の文書を表す文書オブジェクトと、文書構成要素の各セキュリティレベルに対応したセキュリティオブジェクトをディレクトリサービスに登録する。文書オブジェクトには、１以上の文書構成要素が含まれ、この構成要素に対して図２で示したようにセキュリティレベルが設定可能である。

【００５０】そして、本変形例では、セキュリティオブジェクトに対して、開示判定のルールを持たせる。例えば、セキュリティレベル１に対応するセキュリティオブジェクトに、「正社員、担当社員、担当役員に開示可能」などのルールを設定するなどである。セキュリティ

レベル評価部１３０は、印刷対象文書の各構成要素のセキュリティレベルに対応するセキュリティオブジェクトを参照し、このオブジェクトに設定されたルールに従い、印刷ジョブ発行者に対してその構成要素が開示可能かどうかを判断する。

【００５１】この構成の場合、開示範囲を変更する場合には、セキュリティオブジェクトに設定されたルール内容を変更すればよい。例えば、セキュリティレベル１に対応するセキュリティオブジェクトの設定内容を変更すれば、セキュリティレベルが１に設定されている文書構成要素の開示範囲を一括して変更できる。

【００５２】＜変形例２＞次に、ユーザのセキュリティレベルの取得方式の変形例について説明する。この変形例では、ユーザの電子証明書（デジタル証明書）にセキュリティレベルの情報を組み込む。この方式では、ユーザは印刷指示を行う際、プリントシステム１０に対して電子証明書を送り、プリントシステム１０はその電子証明書からそのユーザのセキュリティレベルを取得するというものである。印刷指示の際ユーザ端末２０とプリントシステム１０との間で、ネットスケープ社が提唱するＳＳＬ（Secure Socket Layer）や、インターネット上で仕様が公開されているＴＬＳ（Transport Layer Security:RFC2246）等のセキュア通信方式を用いて通信を行う場合には、セキュア通信路の確立の際に互いの電子証明書が取り交わされる。したがって、ユーザの電子証明書にセキュリティレベルの情報を組み込んでおけば、プリントシステム１０はそのユーザのセキュリティレベルを取得することができる。

【００５３】この方式では、図９に示すようにプリントシステム１０に電子証明書管理部１３５を設ける。なお、図９では省略しているが、この変形例のプリントシステム１０は、電子証明書管理部１３５以外の構成については上記実施形態と同様の機能モジュールを備えている。電子証明書管理部１３５には、所定の認証局が発行した各ユーザの電子証明書が登録されている。そして、システム１０は、電子証明書管理部１３５に電子証明書を登録したユーザしか利用できないようにしている。

【００５４】このシステム１０を用いた場合の処理手順について図９を参照して説明する。

【００５５】Ｓ３０：このプリントシステム１０を利用する場合、ユーザは、プリントシステム１０に対してセキュア通信での接続要求を行い、例えば次のような印刷対象文書のＵＲＩを指定して、印刷指示を発行する。

https://"document-server's address"/path/document.html

【００５６】Ｓ３２：この接続要求により、ユーザ端末と、プリントシステム１０のジョブ受信部１０２との間でセキュア通信路の接続処理が行われ、この接続処理に伴ってユーザの電子証明書がジョブ受信部１０２に送信される。

【００５７】Ｓ３４：ジョブ受信部１０２は、電子証明書を受信すると、電子証明書管理部１３５に対しその電子証明書が正当なものかどうかを問い合わせる。電子証明書管理部１３５は、受信した電子証明書を、保管している当該ユーザの電子証明書と比較し、同じであれば受信した証明書が正当であると判断する。

【００５８】Ｓ３６：このようにしてユーザの電子証明書が正当であると判断されると、ジョブ受信部１０２はジョブ制御部１１４に対してジョブ作成を依頼する。

【００５９】ジョブが作成されると、文書取得部１０４（図９では省略）によりＵＲＩで指定された文書が取得される。このとき、文書取得部１０４はそのＵＲＩを用いて、セキュア通信方式により文書サーバ３０から文書を取得する。このとき、文書取得部１０４は、ユーザの電子証明書を使用することにより、ユーザの代理人として文書取得処理を代理実行する。そして、取得した文書の各構成要素の開示可否を判定する際、ユーザのセキュリティレベルを電子証明書から取得して判定を行う。

【００６０】この変形例では、このように電子証明書に記載されているユーザのセキュリティレベルにより、文書の構成要素の開示可否を決定できる。また、本実施形態では、プリントシステム１０が、要求元ユーザの電子証明書を用いて文書サーバ３０からセキュア通信方式で文書を代理取得するので、プリントシステム１０・文書サーバ３０間の通信路での文書内容の漏洩を防止することができる。

【００６１】また、この変形例では、ユーザからの印刷指示の際にそのユーザの電子証明書を受信しているので、通知部１２２（図３参照）によりそのユーザに対してイベント発生の通知を行う際には、その電子証明書に含まれる当該ユーザの公開鍵を用いて通知内容を暗号化して送信する。これにより、プリントシステム１０からユーザへの通知内容を保護することができる。

【００６２】＜変形例３＞以上の例では、文書のセキュリティ保護処理を、文書サーバ３０から文書を取得するプリントシステム１０の側で行った。これに対し、本変形例では、文書を提供する文書サーバ自体で文書のセキュリティ保護処理を行う例を説明する。ここでは、文書サーバがWWWのＷｅｂサーバであり、Ｗｅｂページをユーザ端末に表示する場合を例にとる。

【００６３】図１０に本変形例におけるＷｅｂサーバ６０の構成を示す。Ｗｅｂサーバ６０は、機能モジュールとして、ＨＴＴＰデーモン６０２、スクリプト実行部６０４、セキュリティレベル評価部６０６、応答文書生成部６０８、及びドキュメントレポジトリ６１０を備える。ＨＴＴＰデーモン６０２は、ユーザからの要求を受け付け、それに応じた応答文書の情報をユーザに送信する。スクリプト実行部６０４は、Ｗｅｂサーバの処理のために必要な各種スクリプトを実行する。ドキュメントレポジトリ６１０は、様々なＨＴＭＬ文書を保存・管理

している。この中には、図２に示したようなセキュリティレベルの設定されたＨＴＭＬ文書も含まれる。応答文書生成部６０８は、ドキュメントレポジトリ６１０から取り出したＨＴＭＬ文書に対し、要求元ユーザのセキュリティレベルに応じた開示内容となるよう編集する。セキュリティ評価部６０６は、ＨＴＭＬ文書の各構成要素のセキュリティレベルとユーザのセキュリティレベルとに基づき、各構成要素ごとに、そのユーザに開示するか否かを判定する。なお、ユーザ端末５０は、一般的なＷｅｂブラウザを備えていればよい。

【００６４】次に、図１１を参照してこのＷｅｂサーバの処理手順を説明する。

【００６５】Ｓ５０：ユーザは、ユーザ端末５０のブラウザから、ＨＴＴＰプロトコルを用いて、Ｗｅｂサーバ６０に対して所望の文書についての文書取得命令を発する。

【００６６】Ｓ５２：Ｗｅｂサーバ６０では、この文書取得命令をＨＴＴＰデーモン６０２が受信し、スクリプト実行部６０４に対しその命令に対する応答文書生成のためのスクリプトを実行させる。

【００６７】Ｓ５４：そのスクリプトの実行により、応答文書生成部６０８に対して応答文書の生成依頼がなされる。

【００６８】Ｓ５６：この依頼に応じ、応答文書生成部６０８は、まず、文書取得命令で指示された文書をドキュメントレポジトリ６０８から取得する。

【００６９】Ｓ５８：そして応答文書生成部６０８は、取得した文書のタグを順に調べていき、セキュリティレベルが設定されている文書構成要素を抽出する。

【００７０】Ｓ６０：セキュリティレベルが設定されている構成要素を見つけると、応答文書生成部６０８はセキュリティレベル評価部６０６に対し、その構成要素の開示性の評価を依頼する。これを受けたセキュリティレベル評価部６０６は、その構成要素のセキュリティレベルと、要求元のユーザのセキュリティレベルとの比較に基づき、それら各構成要素がそのユーザに対して開示できるか否かを判定する。ユーザのセキュリティレベルの情報は、上記実施形態の中に例示した手法で取得できる。この判定において、開示できないと判定された構成要素については、予め設定したセキュリティポリシーに従って、伏せ字や黒塗り画像に置き換えるなどの秘匿処理を行う。例えば、当該ＨＴＭＬ文書において、秘匿すべき文字列の各文字を伏せ字「＊」で置き換えるなどである。このとき、ブラウザの誤動作等を防止するため、セキュリティレベルを示すタグ（Publicityタグ）やパラメータ（Publicityパラメータ）を削除してもよい。取得した文書全体にわたって、このようなＳ５８及びＳ６０の処理を行う。

【００７１】この処理の結果、要求元のユーザに開示できない部分を伏せ字などに置換したＨＴＭＬ文書ができる。このようにしてできたＨＴＭＬ文書が、ＨＴＴＰデーモン６０２から要求元のユーザ端末５０に送信される。

【００７２】ユーザ端末５０では、このようにして取得したＨＴＭＬ文書を通常のブラウザで表示する。この場合、そのユーザが閲覧できないと判定された構成要素は伏せ字置換などで秘匿されており、ユーザはその内容を知ることができない。

【００７３】このように、この変形例では、Ｗｅｂサーバ６０が各ユーザのセキュリティレベルに応じた開示内容のＨＴＭＬ文書を作成してユーザに送る。したがって、ユーザ端末のブラウザに特別な機能がなくても、ユーザに対して開示できない部分を開示しないようにすることができる。

【００７４】以上、本発明の好適な実施の形態とその変形例を説明した。以上説明したように、本実施形態及びその変形例によれば、セキュリティレベル（アクセス権限）の異なる各ユーザに対して、文書の構成要素単位で開示を制御できる。

【００７５】なお、以上では文字や画像の開示制御について説明したが、本発明の手法は、マルチメディア文書等における動画像や音声（サウンド）についても同様に適用可能である。例えばＨＴＭＬ文書には、動画像やサウンドを文書要素として組み込めるが、その要素のタグに例えばPublicityパラメータを設定し、そのパラメータに応じて開示制御を行うことができる。

【００７６】また、以上では、ユーザに提供する文書のフォーマットとしてＨＴＭＬを例にとったが、この本発明の手法は、ＨＴＭＬのみならずＸＭＬ等他のマークアップ言語の文書にも同様に適用可能である。さらに言えば、マークアップ言語以外のフォーマットであっても、文書構成要素ごとに属性情報が設定できるフォーマットであれば、その属性情報の一つとしてセキュリティレベルを設定するようにすることで上記実施形態の手法が適用できる。

【００７７】また以上では、開示できない文書構成要素を秘匿する手法として、予め用意した画像や記号などで置き換える手法を説明したが、秘匿の手法はこのような置換に限らない。例えば、いったん生成したその構成要素の画像に対して平均化フィルタ等の画像フィルタ（元の画像が分からなくなるようなものであればどのようなフィルタでもよい）を作用させて秘匿することも好適である。

【図面の簡単な説明】

【図１】　実施形態の手法が適用されるネットワーク環境の一例を示す図である。

【図２】　構成要素単位でセキュリティレベルが設定されたＨＴＭＬ文書の一例を示す図である。

【図３】　実施形態に係るプリントシステムの機能構成を示す図である。

15　　16

【図４】　実施形態のプリントシステムの機能モジュール間のメッセージ交換手順を示す図である。

【図５】　セキュリティレベル０のユーザに図２の文書を開示した場合の開示結果を示す図である。

【図６】　セキュリティレベル１のユーザに図２の文書を開示した場合の開示結果を示す図である。

【図７】　セキュリティレベル２のユーザに図２の文書を開示した場合の開示結果を示す図である。

【図８】　セキュリティレベル３のユーザに図２の文書を開示した場合の開示結果を示す図である。

【図９】　変形例２のシステムの機能モジュール間のメッセージ交換手順を示す図である。

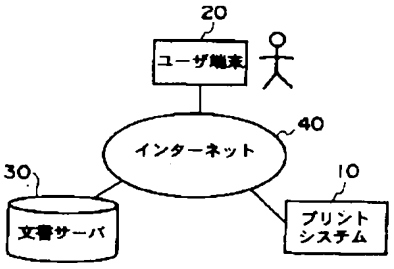
＊【図１０】　変形例３のＷｅｂサーバの機能構成を示す図である。

【図１１】　変形例３のＷｅｂサーバの機能モジュール間のメッセージ交換手順を示す図である。

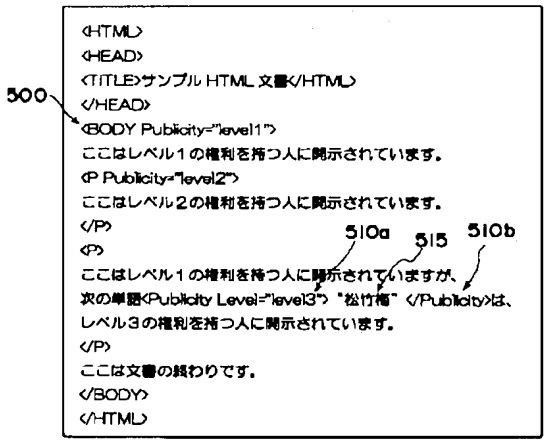
【符号の説明】

１０　プリントシステム、２０　ユーザ端末、３０　文書サーバ、１００　プリントサーバ、１０２　ジョブ受信部、１０４　文書取得部、１０６　スプールバッファ、１０８　文書解析部、１１０　ページバッファ、１１２　出力制御部、１１４　ジョブ制御部、１１６　入力制御部、１１８　タッチパネル、１２０タスク間通信バス、１２２　通知部、１５０　プリントエンジン。

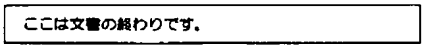
【図１】



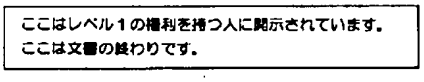
【図２】



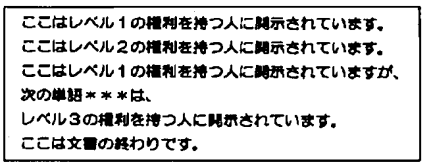
【図５】



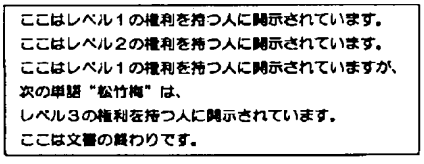
【図６】



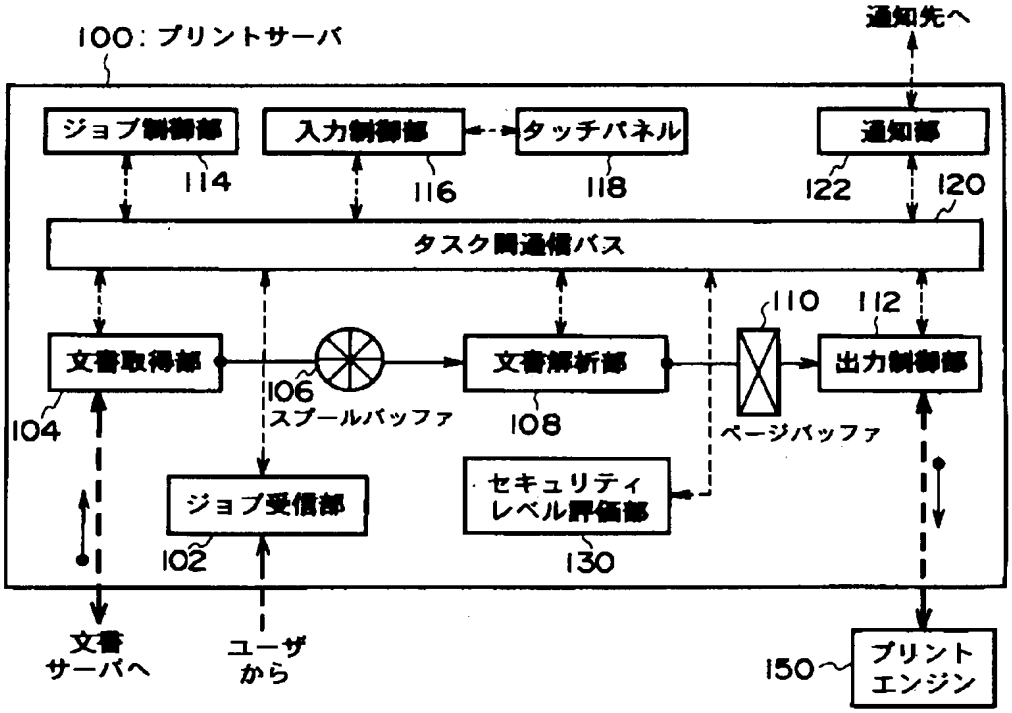
【図７】



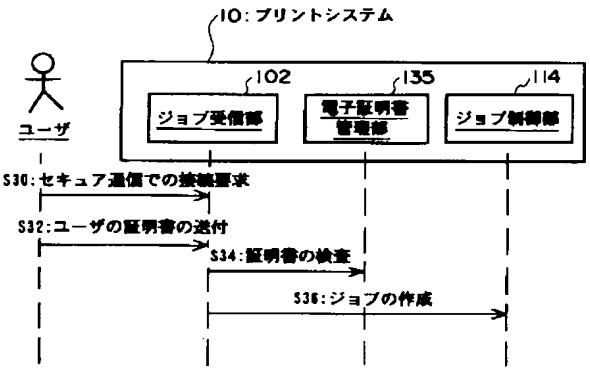
【図８】



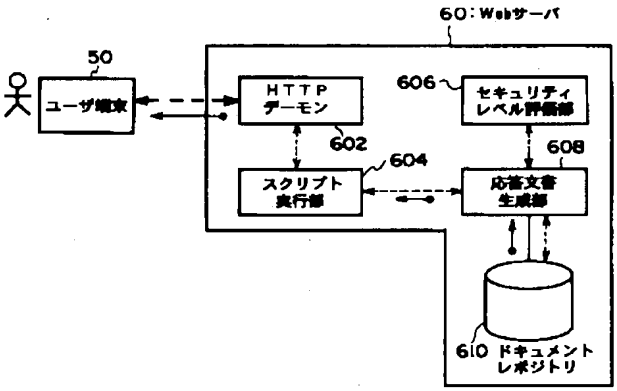
【図３】


100：プリントサーバ
通知先へ
ジョブ制御部
114
入力制御部
116
タッチパネル
118
通知部
122
120
タスク間通信バス
110
112
文書取得部
104
106
スプールバッファ
文書解析部
108
ページバッファ
出力制御部
ジョブ受信部
102
セキュリティ
レベル評価部
130
文書
サーバへ
ユーザ
から
150
プリント
エンジン

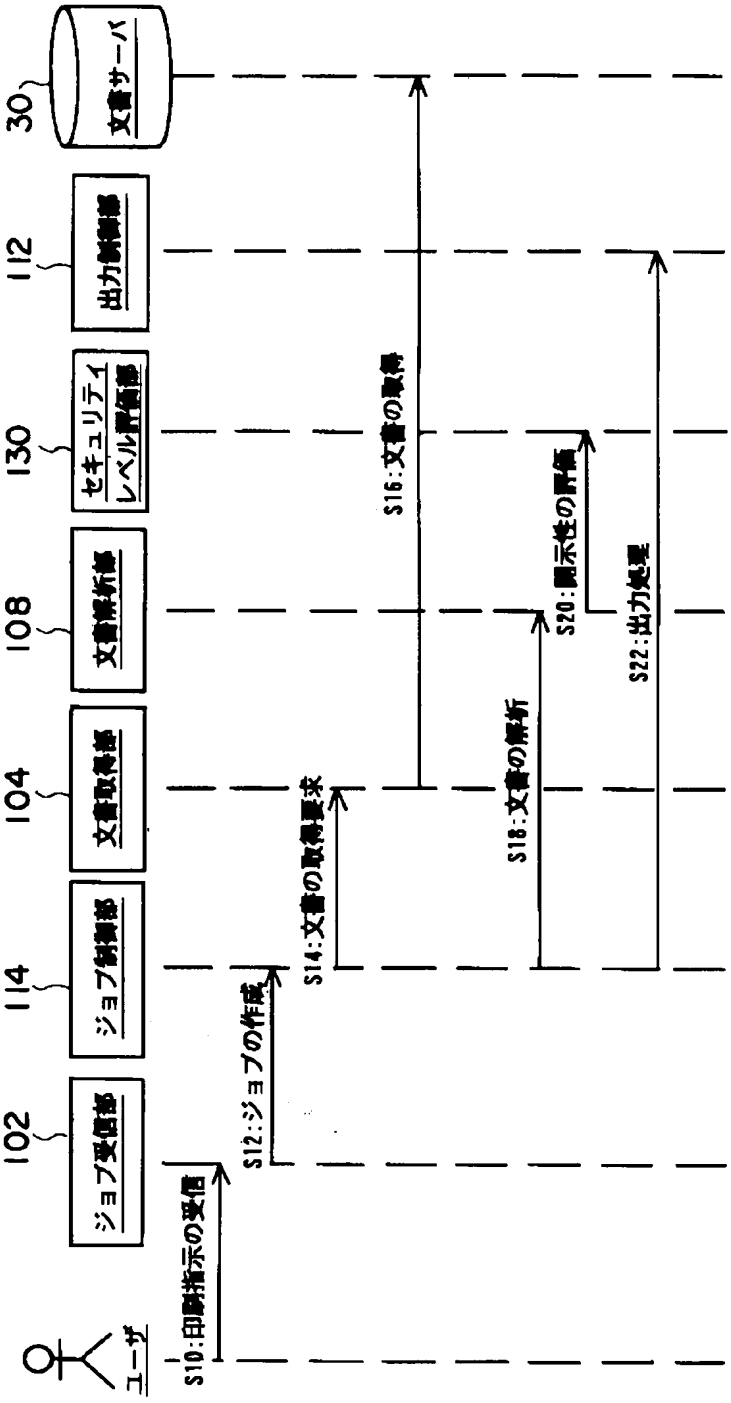
【図９】


10：プリントシステム
ユーザ
102
ジョブ受信部
135
電子証明書
管理部
114
ジョブ制御部
S30：セキュア通信での接続要求
S32：ユーザの証明書の送付
S34：証明書の検査
S36：ジョブの作成

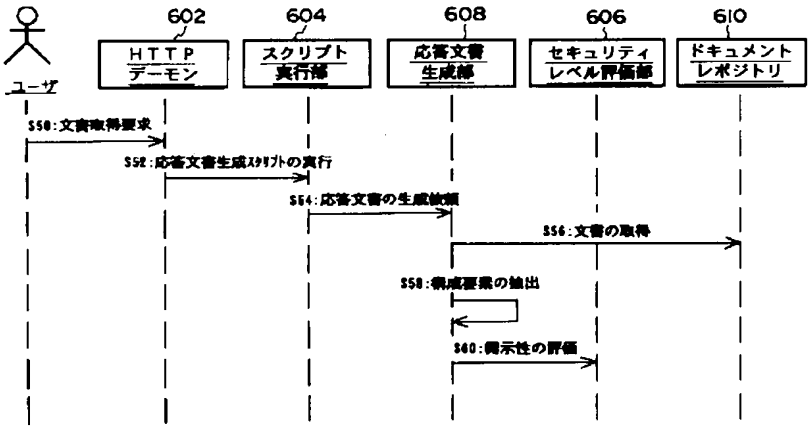
【図１０】


60：Webサーバ
50
ユーザ端末
HTTP
デーモン
602
606
セキュリティ
レベル評価部
608
スクリプト
実行部
604
応答文書
生成部
610 ドキュメント
レポジトリ

【図４】


ユーザ
ジョブ受信部
102
ジョブ制御部
114
文書取得部
104
文書解析部
108
セキュリティレベル評価部
130
出力制御部
112
文書サーバ
30
S10:印刷指示の受信
S12:ジョブの作成
S14:文書の取得要求
S16:文書の取得
S18:文書の解析
S20:開示性の評価
S22:出力処理

【図１１】



フロントページの続き

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ	ﾃｰﾏｺｰﾄﾞ（参考）
Ｇ０６Ｆ　17/30	１７０	Ｇ０６Ｆ　17/30	１７０Ａ